BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
Emily A. Horne (State Bar No. 347723)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
ehorne@bursor.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

VISHAL SHAH and JAYDEN KIM, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

FANDOM, INC.,

Defendant.

Case No. 3:24-cv-01062-RFL

PLAINTIFFS' OPPOSITION TO DEFENDANT'S MOTION TO DISMISS THE FIRST AMENDED COMPLAINT

Date: September 10, 2024
Time: 10:00 a.m.
Courtroom: 15, 18th Floor
Judge: Hon. Rita F. Lin

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

PAGE(S)

CASES

STATUTES

Plaintiffs Vishal Shah and Jayden Kim ("Plaintiffs") respectfully submit this Opposition to Defendant Fandom, Inc.'s ("Fandom" or "Defendant') Motion to Dismiss the First Amended Complaint (ECF No. 20) ("Motion" or "MTD").

INTRODUCTION

When the California Legislature enacted the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.* ("CIPA"), it recognized "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630. Further, as the California Supreme Court has recognized, the intent of the CIPA is to protect the right of Californians to control who does and does not get to learn personal information about them:

> While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device.
>
> …
>
> [S]uch secret monitoring denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements.

Ribas v. Clark, 38 Cal. 3d 355, 360-61 (1985) (cleaned up).

This is the privacy right Defendant breached here. Specifically, when Plaintiffs visited Defendant's website, gamespot.com (the "Website"), Defendant caused third-party trackers operated by third parties—GumGum, Audiencerate, and TripleLift—to be installed on Plaintiffs' and Class Members' web browsers (the "Trackers"). First Amended Complaint (ECF No. 15) ("FAC") ¶¶ 21-23, 36-38, 46-48, 55-58, 66-67, 89-105. Defendant's conduct caused Plaintiffs' and Class Members' personal information—their IP addresses—to be sent to third parties, improperly and without consent. *Id*. An IP address is personal information because it discloses a user's location, which is certainly something users retain the right to choose who knows and who does not. *Id.* ¶¶ 24-31. Further, Defendant's installation of these third-party trackers is not innocuous. Instead, when GumGum, Audiencerate, and TripleLift received Plaintiffs' and Class Members' IP addresses, they

used to bolster Defendant's marketing, advertising, analytics, and revenue-generating efforts. *Id.* ¶¶ 33-35, 42-45, 52-54, 73-88.

To put the allegations in the FAC as succinctly as possible, Plaintiffs allege Defendant installed third-party trackers on Plaintiffs' and Class Members' browsers, which caused Plaintiffs' and Class Members' location (via their IP addresses) to be sent to third parties (without consent), and that Defendant partnered with these third parties to enrich itself off of this improperly disclosed information (without compensation or consent). Plaintiffs allege Defendant's conduct violates CIPA § 638.51, which prohibits the unconsented-to installation and use of "pen registers" and "trap and trace devices."

Though Defendant raises a bevy of legal arguments in its Motion, not once does Defendant dispute the underlying conduct: that Defendant installed trackers that disclosed users' IP addresses to third parties, and did so for marketing, advertising, and revenue-generating purposes. And for the reasons set forth below, each of Defendant's arguments is without merit, and its Motion should be denied.

ARGUMENT

I. DEFENDANT'S MOTION FAILS TO COMPLY WITH THE COURT'S INDIVIDUAL RULES

Right out of the gate, Defendant's Motion stumbles based on Defendant's failure to comply with the Court's Individual Rules. Specifically, the Court requires all filings to be made "by 5:00 p.m. (Pacific Time)." Standing Order For Civil Cases Before Judge Rita F. Lin, at 4.1 In addition, while the Court permits "25 pages" of briefing for certain motions, briefing on all other motions—including a motion to dismiss— "may not exceed 15 pages." *Id.* at 6. As courts have noted, "page limits are not mere formalities. They are important. Page limits promote judicial economy and "encourage litigants to hone their arguments and to eliminate excessive verbiage." *LaComba v. Eagle Home Loans and Investment, LLC*, 2023 WL 6201597, at *1 (E.D. Cal. Sept. 22, 2023) (striking overlength briefs).

[1] Available at https://www.cand.uscourts.gov/wp-content/uploads/2023/03/2024-05-17-Civil-Standing-Order.pdf.

Here, Defendant's Motion is nineteen pages and was filed at 8:43 p.m. Pacific Time. Further, Defendant did not file a request for a page extension. Accordingly, Plaintiffs respectfully request that the Court either (i) strike the final five pages of Defendant's Motion as overlength, (ii) require Defendant to file a version of its Motion that is *not* overlength, or (iii) limit Defendant's Reply Brief to five (5) pages, rather than ten. *See*, *e.g.*, *Swanson v. U.S. Forest Serv.*, 87 F.3d 339, 345 (9th Cir. 1996) (affirming district court's decision to strike an overlength brief)

II. DEFENDANT IS LIABLE FOR INSTALLING PEN REGISERS ON PLAINTIFFS' DEVICES, WHICH CAUSED THEIR IP ADDRESSES TO BE SENT TO THIRD PARTIES

Defendant argues "Section 638.51(a) does not apply to Fandom's collection of [] IP address[es]" because users "necessarily and voluntarily disclose[]" this data "to visit the website." MTD at 5. Defendant misunderstands or misconstrues Plaintiffs' allegations. Plaintiffs' claim is *not* that their IP addresses were disclosed to Defendant. Instead, Plaintiffs' claim is that Defendant installed "pen registers" (the Trackers) on their browsers, which caused Plaintiffs' IP addresses to be sent to third parties. FAC ¶¶ 2, 21-23, 32, 38, 41, 48 50, 57, 60, 70, 78, 83, 88, 89, 118, 120. Whether sharing Plaintiffs' IP addresses is required to operate the Website, there is nothing "necessary" about disclosing Plaintiffs' IP addresses to third parties who use the information for marketing, advertising, and data analytics. As the California Supreme Court has held, this accords with the purpose of CIPA:

> While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device.
>
> …
>
> [S]uch secret monitoring denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements.

Ribas, 38 Cal. 3d at 360-61. Thus, the claim here is that third parties simultaneously and improperly acquired Plaintiffs' IP addresses through Defendant's installation of pen registers, *not* that Defendant itself acquired Plaintiffs' IP addresses.

Defendant's cited authorities are all distinguishable on this basis. For instance, in *Licea v. Hickory Farms LLC*, 2024 WL 1698147 (Cal. Super. March 13, 2024), the plaintiff did *not* allege

the defendant shared IP addresses with a third party. First Amended Complaint, *Licea v. Hickory Farms LLC*, Case No. 23STCV26148, 2023 WL 11113637 (Cal. Super. Dec. 4, 2023). Instead, the plaintiff alleged that the defendant "knowingly and intentionally deployed a software device" on to its own website for its own "identity resolution efforts." *Id.* ¶ 17. Thus, the *Licea* court reasoned there was "consent under the guise of visiting a website," because the defendant could not otherwise be able to host a website. *Licea*, 2024 WL 1698147, at *4. Here, however, Plaintiffs allege Defendant installed a pen register that disclosed their information to *third parties*. *See*, *e.g.*, FAC ¶ 23.

Similarly, the federal court decisions Defendant cites are distinguishable. In *Capitol Records Inc. v. Thomas-Rasset*, 2009 WL 1664468, at *3 (D. Minn. June 11, 2009), in addition to the user consenting to the disclosure of the IP address, the court held "the Pen Register Act cannot be intended to prevent individuals who receive electronic communications from recording the IP information *sent to them*." (Emphasis added). But again, Plaintiffs' claim is not that their IP addresses were sent to Defendant, the only entity with whom Plaintiffs were directly communicating. *See also id.* ("MediaSentry, as a party to th[e] communication, simply recorded the information transmitted to it from Thomas–Rasset's computer."). Likewise, in *Malibu Media, LLC v. Pontello*, 2013 WL 12180709 (E.D. Mich. Nov. 19, 2013), the IP address was also sent to the other party to the communication, not a third party. *Id.*, at *4 ("By participating in the BitTorrent swarm Pontello consensually engaged in the transaction with IPP, and communicated his IP address as part of the packet his computer sent to IPP.").

Finally, Defendant attempts to distinguish *Greenley v. Kochava*, 684 F. Supp. 3d 1024 (S.D. Cal. Jul. 27, 2023), yet their argument is unpersuasive. There, the defendant was a data broker that provided software developer kits ("SDK") to software developers to assist in developing apps. *Id.* at 1035. Defendant coded its SDK for data collection and embedded it in third-party apps, the SDK collected app users' data, and then defendant sold that data to clients for advertising purposes. *Id.* Defendant argues, unlike *Greenley*, Fandom only collected and shared data that "was already necessarily communicated to Fandom." MTD at 9. Despite Defendant's contention, like *Greenley*, it was *not* necessary for Defendant to disclose Plaintiffs' IP address to third parties for the Website

to function. Defendant also argues this case is distinguishable because the *Greenley* defendant was a third-party data broker that provided the software to developers, whereas, here, Defendant owns and operates the Website and does not operate the Trackers. MTD at 9. On the contrary, the third parties here, like the *Greenley* defendant, used the improperly collected user information for marketing, advertising, or data analytics purposes without the users' consent.[2] And the pen register statute penalizes those who *install* or use pen registers, which Defendant did. Cal. Penal Code § 638.51(a); *see also*, *e.g.*, FAC ¶¶ 23, 32. Third party code does not appear on the Website by accident, it must be affirmatively placed on the Website and programmed by Defendant. *See id*.

Accordingly, Plaintiffs' claim is distinguishable from both the California and federal court cases Defendant cites. Plaintiffs do not allege Defendant violated CIPA by collecting users' IP addresses. Rather, Plaintiffs allege Defendant violated CIPA by disclosing users' IP addresses to third parties via the Trackers it installed without users' consent.

III. THE TRACKERS ARE PEN REGISTERS

Defendant argues CIPA § 638.51 does not apply because the Trackers are not "pen register[s]." MTD at 9. To the contrary, the Trackers are pen registers that Defendant installs and uses in violation of CIPA. Further, Defendant's narrow reading of the statute is contrary to the statute's plain text and the California Legislature's intent.

A. The Trackers Are Pen Registers Because They Collect Outgoing Information

Defendant suggests that "pen registers" are intended to "enable[] law enforcement officers to identify the persons to whom targeted individuals in a criminal investigation are speaking," and thus the Trackers cannot be pen registers. MTD at 10. This is the exact reason CIPA § 638.51 provides for an exception for law enforcement and does not allow companies—such as Defendant—to collect and share such identifying information. *See* Cal. Penal Code § 638.52(a). The California Legislature intended for law enforcement to surveille individuals, not companies to enable third parties to surveille consumers.

[2] The court in *Casillas v. Transitions Optical, Inc.*, Case No. 23STCV30724 (Cal. Super. April 23, 2024) (filed as Jones Decl., Ex. 10 (ECF No. 20-11)) did not analyze *Greenley* in depth. Instead, the court sustained the demurrer because "the Complaint ma[de] inappropriate and conclusory legal arguments" and "allege[d] few ultimate facts." *Id.*

Defendant next contends the Trackers are not pen registers because an IP address is not "outgoing information" under CIPA § 638.50(b). MTD at 10-11. As an initial matter, the federal pen register statute encompasses IP addresses—regardless of whether it is the individual users' IP address (*i.e.*, sender) or the visited website's IP address (*i.e.*, recipient). Indeed "an IP pen register is analogous in all material respects to a traditional telephone pen register." *United States v. Soybel*, 13 F.4th 584, 594 (7th Cir. 2021); *see also*, *United States v. Ulbricht*, 858 F.3d 71, 97 (2d Cir. 2017) (holding the "recording of IP address … [is] precisely analogous to the capture of telephone numbers"), *abrogated on other grounds*, *Carpenter v. United States*, 585 U.S. 296 (2018). Given CIPA was, in part, modeled after the federal wiretap act—which includes the federal pen register statute—such caselaw is instructive. *Underhill v. Kornblum*, 2017 WL 2869734, at *6 (S.D. Cal. Mar. 16, 2017) ("The analysis for a violation of CIPA is the same as that under the federal Wiretap Act.").

Further, although CIPA was enacted before the Internet was created, "the California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." *In re Google Inc.*, 2013 WL 5423918, at *21 (N.D. Cal. Sept. 26, 2013). "For example, in a previous evolution in communications technology, the California Supreme Court interpreted 'telegraph' functionally, based on the type of communication it enabled." *Id.* "In *Davis v. Pacific Telephone & Telegraph* [127 Cal. 312, 316 (Cal. 1899)], the Supreme Court held that '*telegraph* lines' … included *telephone* lines because 'the idea conveyed by each term is the sending of intelligence to a distance … thus the term 'telegraph' means any apparatus for transmitting messages by means of electric currents and signals." *Id.* (emphasis in original). In addition, the Ninth Circuit has noted that "[t]hough written in terms of wiretapping, [CIPA] applies to Internet communications." *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022).

Here, the statute defines a "pen register" as a "device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b). Put differently, a pen register records the "outgoing" information from a person that is being surveilled. FAC ¶¶ 14-16. And an IP address at least constitutes "routing,

addressing, or signaling information" because it identifies a specific device and divulges a user's location. *Id.* ¶¶ 24-28. Accordingly, the collection of IP addresses by third parties falls within the purview of CIPA § 638.50(b).

Defendant's arguments are unpersuasive. *First*, Defendant argues the statute cannot cover a user's IP address because the information is about the user rather than the "*recipient* [of the] information of the outbound communication." MTD at 11 (emphasis in original). However, the statute does not limit *who* the recorded information must regard. Cal. Penal Code § 638.50(b). Regardless, CIPA is intended to "protect the right of privacy of the people of this state from what it perceived as a serious threat to the free exercise of personal liberties that cannot be tolerated in a free and civilized society." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 775 (2002) (cleaned up). As the California Supreme Court explained, "[t]his philosophy appears to lie at the heart of virtually all the decisions construing [CIPA]." *Id.* Thus, the CIPA was intended to protect those who make calls or communicate over the internet and have their information disclosed, not to protect those who are on the receiving end of this information.

Second, Defendant contends the collection of IP addresses does not fall within the statute because it is the "source of a communication." MTD at 13. Even if Defendant were correct (it is not), this would just mean the Trackers are "trap and trace devices," which also cover "electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication." Cal. Penal Code § 638.50(c). Indeed, pen registers and trap and trace devices are almost always used together, and thus, courts generally discuss them as one. *See*, *e.g.*, *Soybel*, 13 F.4th 584, 586 n.2 (7th Cir. 2021) ("For the sake of simplicity, we use the term "pen register" to refer to both [pen registers and trap and trace devices]."). An IP address also fits within this definition. So, one way or another, Defendant is violating the CIPA.

Third, Defendant is wrong that CIPA § 638.50 categorically excludes IP addresses. MTD at 14. Instead, various sections of CIPA protect against a range of data, such as "a patient's identity in the form of cookies, *IP address*, and User-Agent identifiers," *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 785 (N.D. Cal. Dec. 22, 2022) (emphasis added); a user's browsing history, *In re*

Facebook, 956 F.3d at 606-08; and even mouse clicks and keystrokes. *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 517-18 (C.D. Cal. 2021).[3] And, as noted above, the federal pen register statute has been held to apply to IP addresses. *Soybel*, 13 F.4th at 594; *Ulbricht*, 858 F.3d at 97.

Accordingly, the Trackers are pen registers because they capture website visitors' IP addresses, which are "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." Cal. Penal Code § 638.50(b).

B. IP Addresses Are Not "Content" As Defined By CIPA

Defendant claims the Trackers cannot be pen registers because they "collect the contents of a communication" and not the "dialing, routing, addressing, or signaling information of a communication." MTD at 14. This is wrong. "The term 'contents' refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication." *Saleh*, 562 F. Supp. 3d at 517 (citing *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014)); *see also* 18 U.S.C. § 2510(8) (defining "contents" for the Federal Wiretap Act as "includ[ing] any information concerning the substance, purport, or meaning of that communication"). As the Ninth Circuit has held, "IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication." *In re Zynga Priv. Litig.*, 750 F.3d at 1106 (cleaned up); *In re Nickelodeon Consumer Priv. Litig.*, 2014 WL 3012873, at *15 (D.N.J. July 2, 2014) ("IP addresses and URLs" are not content).

Here, Plaintiffs specifically allege that the Trackers *only* collect customer record information—in this case, IP addresses, which are "dialing, routing, addressing or signaling information"—but "do not collect the content of Plaintiffs' and the Class's electronic communications with the Website." FAC ¶¶ 117-119. Accordingly, the Trackers are pen registers

[3] Defendant's reliance on *In re the Application of the U.S. for an Ord. Authorizing the Installation & Use of a Pen Reg. & Trap & Trace Device*, 890 F. Supp. 2d 747 (S.D. Tex. 2012) is unpersuasive. There, the court denied a pen register application by the U.S. Attorney's Office because the application did not sufficiently explain how the technology would be used to engage in surveillance. *Id.* at 749, 752. Here, Defendant cannot request authority to surveille consumers under CIPA because there is no exception for non-government entities.

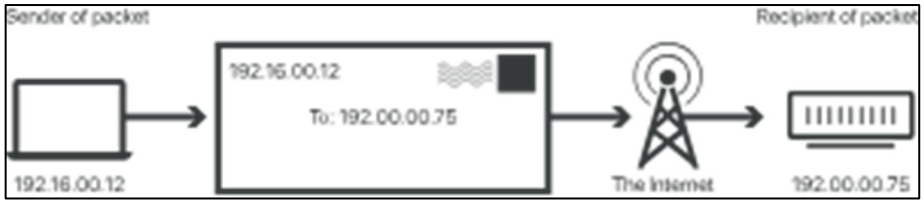
because they only collect IP addresses, which are "dialing, routing, addressing or signaling information," but *not* content.

Defendant's arguments are unpersuasive. *First*, Defendant contends Plaintiffs have not identified any "communications" that were intercepted. MTD at 14. As an initial matter, the pen register statute requires interception of "dialing, routing, addressing or signaling information … but not the contents of a communication." Cal. Penal Code § 638.50(b). Thus, the statute does not require the collection of a communication. Regardless, Plaintiffs' accessing of the Website is a communication within the meaning of the CIPA. *See Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *1 (N.D. Cal. Oct. 23, 2019) ("Revitch requested information from Moosejaw by clicking on items of interest; Moosejaw responded by supplying that information. This series of requests and responses – whether online or over the phone – is communication.").

Second, Defendant contends that because an IP address is sometimes collected by the Trackers through a cookie (as opposed to directly), the Trackers collect "the content of communications" because the IP address is the "content" of the cookie transmission. MTD at 15 (cleaned up). This argument makes no sense. An IP address still does not divulge the "substance, purport, or meaning" of a communication (18 U.S.C. § 2510(8)), and so cannot be "content" within the meaning the CIPA even if it is the only information being transmitted.

Further, the mechanism through which the IP address is sometimes transmitted—the cookie—is irrelevant to whether the IP address is content, and even supports Plaintiffs' allegations. Picture the cookie transmission as someone mailing a letter to a friend, with addressing information on the letter. If the friend never opens the letter but reads the outside, they learn the addressing information of the send, but *not* the content of the letter (*i.e.*, the content of the communication). In that analogy, the cookie is the unopened letter and the IP address is the addressing information on the front. Thus, no content is divulged to the Trackers (nor does Plaintiffs allege as much).[4]

[4] WHAT IS THE INTERNET PROTOCOL (IP)?, https://www.cloudflare.com/learning/network-layer/internet-protocol/.



Regardless, an IP address does not magically become content because it is the only information disclosed; it is still "record information regarding the characteristics of the message that is generated in the course of the communication." *Saleh*, 562 F. Supp. 3d at 517

Defendant cites *Capitol Recs. Inc.* and *Malibu Media, LLC* to show that Defendant's collection of IP addresses is incidental to—or part of—its process of collecting the content of communications, but neither case is availing here. In *Capitol Recs. Inc.*, 2009 WL 1664468, at *3, IP addresses were "transmitted along with every file sent through the FastTrack network," whereas in *Malibu Media, LLC*, 2013 WL 12180709, at *4, the plaintiff "communicated his IP address as part of the packet his computer sent to" defendant's investigators. Here, in contrast, Plaintiffs are neither transmitting files that incidentally share their IP addresses, nor deliberately communicating their IP addresses as part of a larger packet of information sent to third parties. And Plaintiffs never allege the contents of any communications were transmitted to the third-party Trackers. Defendant's argument that Plaintiffs' IP addresses are part of the contents of larger communications "between Plaintiffs' browsers and third-party servers" therefore fails. MTD at 15.

IV. CIPA § 638.51 COVERS INTERNET BASED COMMUNICATIONS

Defendant argues CIPA § 638.51(a) "applies only to 'device[s] or process[es]' used for *telephone* surveillance and tracking," and "does not apply to software that collect the source IP address from a user's computer." MTD at 15 (emphasis in original). This is wrong. The Ninth Circuit has explained that "[t]hough written in terms of wiretapping, [CIPA] applies to Internet communications." *Javier*, 2022 WL 1744107, at *1; *see also*, *e.g.*, *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 936 (N.D. Cal. Oct. 23, 2015) (noting that courts have "squarely rejected" the argument that CIPA "should be narrowly construed and should not be applied to electronic communications"). This comports with the broad language of CIPA § 638.50(b), which defines "pen register" as a "device or process that records or decodes dialing, routing, addressing, or signaling

information transmitted by an instrument or facility from which a wire *or electronic communication* is transmitted." (emphasis added). It also comports with the fact that "the California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." *In re Google Inc.*, 2013 WL 5423918, at *21. And it comports with the fact that "the California legislature intended for CIPA to establish broad privacy protections [which] supports an expansive reading of the statute." *Id.*; *see also Flanagan*, 27 Cal. 4th at 775 ("In enacting [CIPA], the Legislature declared in broad terms its intent to protect the right of privacy of the people of this state from what it perceived as a serious threat to the free exercise of personal liberties that cannot be tolerated in a free and civilized society.") (cleaned up).

Defendant further argues CIPA § 638.51 applies solely to telephonic surveillance as explained by *Licea v. Hickory Farms LLC*. MTD at 15. This is incorrect. In *Licea*, 2024 WL 1698147, at *4, the court ruled that plaintiff's claim "lacked factual support [] under the [demurrer] standard." The deficiency of the claim did not hinge on whether the alleged pen register device was a telephonic device. Rather, the deficiency of the claim was the result of a "conclusively pled complaint." *Id.*, at *4. Here, in contrast, Plaintiffs avoid conclusory pleadings by alleging that each Tracker installed by Defendant captures users' IP addresses, how that data is shared with third parties, and why that violates CIPA. *See* FAC ¶¶ 1-5, 89-105. Moreover, as discussed above, the federal pen register statute has been repeatedly applied to the collection of IP addresses. *Soybel*, 13 F.4th at 594; *Ulbricht*, 858 F.3d at 97. Thus, to the extent *Licea* stands for the proposition Defendant cites it for (it does not), *Licea* contravenes well-established law.

Next, Defendant asserts *Greenley* supports its argument because it involved a mobile device rather than a computer. MTD at 17. That makes no sense. The case involved a mobile application using internet connectivity on the mobile device. *Id.* 1037. It had nothing to do with "phone technology." Moreover, other cases have regularly applied CIPA to computer-based internet wiretapping. *See Revitch*, 2019 WL 5485330, at *2 ("Revitch began each communication by pressing a button on his mouse or a key on his keyboard, causing one signal to travel to his computer and then through his browser to Moosejaw's server."); *Matera v. Google Inc.*, 2016 WL 8200619, at *3, 21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to email, "not just to communications passing over

telephone and telegraph wires, lines, or cables"); *In re Google Inc.*, 2013 WL 5423918, at *21 ("In line with the plain language of the statute, the California Supreme Court's pronouncements regarding the broad legislative intent underlying CIPA to protect privacy, and the California courts' approach to updating obsolete statutes in light of emerging technologies, the Court finds that section 631 of CIPA applies to emails"). And again, the Ninth Circuit broadly declared "[t]hough written in terms of wiretapping, [CIPA] applies to Internet communications." *Javier*, 2022 WL 1744107, at *1.

Defendant also attempts to distinguish *Greenley* because it involved a "complex software that collected a multitude of user data" used to uniquely "fingerprint" each user, whereas Plaintiffs' allegations here only concern IP addresses whose use for "unique fingerprinting" is "pure speculation." MTD at 17 (quoting *Greenley*, 684 F. Supp. 3d at 1050). Notwithstanding none of this has to do with whether the software in *Greenley* was a pen register, the use of IP addresses to "fingerprint" users is not speculative. It is well known IP addresses are "unique numerical code[s] associated with a specific internet-connected device" and that knowing a user's IP address is akin to knowing a user's geographical location. FAC. ¶ 27. Plaintiffs also allege an IP address can be used to hyper-target consumers. *Id.* ¶¶ 28-31. Similarly, Defendant tries to distinguish *Greenley* because that defendant "collected a multitude of user data" which implicates CIPA § 638.51, whereas here Fandom only shares users' IP addresses. MTD at 17. Just like *Greenley*, the "information amassed [by the Trakcers] is [] revealing, and the method is [] secretive," and thus CIPA § 638.51 is implicated. *Greenley*, 684 F. Supp. 3d at 1047. If the emphasis, per the *Greenley* court, is "less on the form of the data collector and more on the result," then the software used here, which collects information sufficient to identify devices and locate users, also falls under the purview of CIPA § 638.51. *Id.*

V. PLAINTIFFS SUFFICIENTLY ALLEGE DEFENDANT INSTALLED AND USED THE TRACKERS

Defendant argues the FAC "should also be dismissed for the separate reason that Plaintiffs fail to plausibly allege that Fandom "install[ed] or use[d] the alleged pen register." MTD at 18. This is not true. Plaintiffs allege in detail, with illustrative figures, how Defendant installed the alleged pen register devices without Plaintiffs' consent. FAC ¶¶ 21-23, 36-38, 46-48, 55-58, 66-67, 89-105.

These allegations are sufficient to survive a motion to dismiss, as Plaintiffs need only "allege 'enough facts to state a claim to relief that is plausible on its face.'" *Gershzon v. Meta Platforms, Inc.*, 2023 WL 5420234, at *4 (N.D. Cal. Aug. 22, 2023) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)).

Defendant claims the FAC "focuses on the action of third parties GumGum, Audiencerate, and TripleLift and never addresses the fundamental question why Fandom would install or use the [Trackers]." MTD at 18. This characterization of Plaintiffs' FAC ignores Plaintiffs' allegations. As an initial matter, third party software code did not magically appear on the Website. Defendant had to specifically configure the Website to cause the Trackers to be installed on Plaintiffs' and Class Members' browsers. FAC ¶¶ 21-23. Moreover, Plaintiffs allege how the pen registers "collect[] users' IP addresses … so that Defendant can analyze user data, create and analyze the performance of marketing campaigns, and target specific users or specific groups of users for advertisements. All of this helps Defendant further monetize its Website and maximize revenue by allowing third parties to collect user information." FAC ¶¶ 78, 88; *see also id.* ¶¶ 73-77, 79-87.

Defendant further tries to analogize the allegations here to those in *Esparza v. Lenox Corp.*, 2023 WL 2541352 (N.D. Cal. Mar. 16, 2023), but such a comparison is inapposite. In *Esparza,* plaintiff made "a passing reference to a 'third-party vendor' … but does not allege what service the vendor provides let alone how or why this alleged vendor interacts with defendant." *Esparza*, 2023 WL 2541352, at *3. Here, in contrast, Plaintiffs describe exhaustive detail the services provided by third party vendors—GumGum, Audiencerate, and TripleLift—in addition to illustrating Defendant's installation of the Trackers and use of the Trackers to monetize its Website. *See* FAC ¶¶ 32-61, 73-88.

Defendant also claims Plaintiffs "fail to plead sufficient facts to nudge the FAC from Fandom *possibly* installing or using the [Trackers], to *plausibly* doing so." MTD at 18 (emphasis in original). Yet Plaintiffs offer multiple allegations describing how "Defendant's server sends an HTTP response with directions to install" the Trackers, and provide illustrative figures that clearly show Plaintiffs' IP addresses being transmitted to the three Trackers. *See* FAC ¶¶ 33-61 (Figures 3-6). Plaintiffs' allegations detailing the installation process, as well as its screenshots showing the transmission of

IP addresses to and through the third-party Trackers, nudge the allegations over the line from possible to plausible. Last, there is no alternative rationale for the existence of these Trackers on Defendant's Website other than Defendant's own installation of them for advertising and marketing purposes. Again, third party code does not just appear on Defendant's Website by magic.

VI. THE AMENDED COMPLAINT SHOULD NOT BE DISMISSED WITH PREJUDICE

Should the Court grant Defendant's Motion (which it should not), the FAC should not be dismissed with prejudice. Despite Defendant's assertion that Plaintiffs' claim is futile (which it is not), the Ninth Circuit has consistently granted plaintiffs leave to amend regardless of multiple previously amended pleadings. *See Roney v. Miller*, 705 F. App'x 670, 671 (9th Cir. 2017) (holding lower court erred in denying leave to amend after dismissing first amended complaint); *United States v. United Healthcare Ins. Co.*, 848 F.3d 1161, 1183 (9th Cir. 2016) (reversing denial of leave to amend even though the plaintiff had previously amended his pleading three times). This is especially true where, as here, the Court has not yet ruled on the merits of Defendant's arguments or Plaintiffs' allegations.

Furthermore, despite Defendant's assertion, the Ninth Circuit has emphasized "[u]nder futility analysis, dismissal without leave to amend is improper unless it is clear, upon *de novo* review, that the complaint could not be saved by any amendment." !!*United States v. Corinthian Colleges*, 655 F.3d 984, 995 (9th Cir. 2011) (cleaned up); *see also Lopez v. Smith,* 203 F.3d 1122, 1130 (9th Cir. 2000) (noting that a court should permit amendment "unless it determines that the pleading could not possibly be cured by the allegation of other facts"). Should the Court decide to grant Defendant's Motion, Plaintiffs should be granted leave to amend to cure defects in the allegations.

CONCLUSION

For the foregoing reasons, the Court should deny Defendant's Motion in its entirety. If the Court grants the Motion in any respect, Plaintiff respectfully requests leave to amend. *See Roney*, 705 F. App'x at 671; *United Healthcare Ins. Co.*, 848 F.3d at 1183.

Dated: June 28, 2024

Respectfully submitted,

BURSOR & FISHER, P.A.

By: /s/ *L. Timothy Fisher*
L. Timothy Fisher

L. Timothy Fisher (State Bar No. 191626)
Emily A. Horne (State Bar No. 347723)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
ehorne@bursor.com

Attorneys for Plaintiffs